



EAMS Present Term Solution (PTS) Technical Specifications - Bulk Filing V2.0

Department of Industrial Relations
Electronic Adjudication Management System

June 16, 2010



**EAMS Application
Development and Maintenance**



Revision History

Date	Version	Description	Author
02/05/10	1.0	Initial Version	CKV Sadishkumar – EAMS IT
02/15/10	1.1	Use Case updates	CKV Sadishkumar – EAMS IT
02/17/10	1.2	Layout updates	CKV Sadishkumar – EAMS IT
02/24/10	1.3	1. Section 3.1 Introduction and chart updates 2. Appendix A Terminology additions/updates	Susan Gard – DWC
02/25/10	1.4	1. Section 3.4 Submitter Use Cases 2. Section 4.4 Canonical Model 3. Section 5 Error Messages	CKV Sadishkumar – EAMS IT Ira Philips – EAMS IT Nina Kot, Jackie Chang – EAMS IT
05/6/10	2.0	1. Technical Specifications divided into 2 documents: - Bulk Filing (V2.0) - All other technical activities	CKV Sadishkumar – EAMS IT Ira Philips – EAMS IT Nina Thayer – EAMS IT
05/7/10- 06/7/10	2.0	Revision of Bulk Filing (V2.0) Technical Specifications	CKV Sadishkumar – EAMS IT Ira Philips – EAMS IT Nina Thayer – EAMS IT Dale Klein – EAMS IT

Table of Contents

EAMS Present Term Solution (PTS) Technical Specifications - Bulk Filing V2.0	1
June 16, 2010	1
1 Introduction.....	5
1.1 Purpose.....	6
1.2 Scope.....	6
1.3 References – Documents Reside at New PTS Web Page.....	6
2 Present Term Solution (PTS)	7
2.1 SFTP Bulk Filing	8
2.1.1 Overview.....	8
2.2 Present Term Solution – “Must Have” Requirements.....	9
3 SFTP Bulk Filing Requirements and Technical Use Cases	12
3.1 EAMS SFTP Bulk Filing -- Business Rules	12
3.1.1 EAMS PTS Business Rules	12
3.2 EAMS SFTP Bulk Filing -- Technical Use Cases	29
3.2.1 Transmission Acknowledgment and Responses	29
3.2.2 EAMS Batch Process	31
3.2.3 SFTP Transmission.....	32
3.2.4 Transaction Layouts	33
3.2.5 Other Technical Activities	33
3.3 Submitter SFTP Bulk Filing -- Technical Use Cases	34
4 XML Layout Specifications and Schema Definitions.....	36
4.1 Payload Layout	37
4.1.1 SubmitFormsToEAMS Layout.....	39
4.1.2 EAMSFilingResponse Layout.....	41
4.1.3 EAMSPacketReceiveResponse Layout	44
4.1.4 EAMSPacketValidationResponse Layout	44
4.2 DWCPacket Layout	46
4.3 Forms Specifications	48
4.4 Canonical Data Model	48
4.5 Schema Definitions.....	50
5 Error Codes and Messages.....	51
5.1 Level 1 Error Messages.....	52
5.2 Level 2 Error Messages.....	53
5.3 Level 3 Error Messages.....	53
5.4 Error Codes and Messages Table	54
6 Present Term Solution (PTS) Security	65
6.1 SFT Overview	65
6.2 Infrastructure Security – Office of Technology Services (OTech) Security Standard	65
6.3 Infrastructure Security – Present Term Solution.....	65
7 Guidelines and Standards	67
7.1 Technical Guidelines	67
7.1.1 Form Guidelines	67
7.1.2 Transaction Guidelines.....	68
7.1.3 Payload Guidelines	69
7.1.4 Transmission and DWCPacket Guidelines	69
7.1.5 Exception Handling Guidelines	70
7.2 XML Schema Standards.....	70
7.2.1 General Schema Guidelines	71
7.2.2 Standard Elements.....	71
7.2.3 Field Restrictions	71
7.2.4 Section Names	72
Appendix A: PTS Project Terminology/Descriptions.....	73
Appendix B: EAMS Access Business Requirements List	79

Appendix C: EAMS Access Business Use Case Statements.....	79
Appendix D: SFTP Forms-ID Mapping	79
Appendix E: SFTP Forms Layout Specifications	79

List of Tables

Table 1: EAMS Access “Must Have” Requirements	11
Table 2: EAMS Business Rules List	29
Table 3: EAMS Technical Use Cases List – Acknowledgment.....	30
Table 4: EAMS Technical Use Cases List – EAMS Batch Process.....	32
Table 5: EAMS Technical Use Cases List – SFTP Transmission	32
Table 6: EAMS Technical Use Cases List – Layout	33
Table 7: EAMS Technical Use Cases List – Others	34
Table 8: Submitters Technical Use Cases List	35
Table 9: SubmitFormsToEAMS Payload Layout	41
Table 10: EAMSFilingResponse Layout	43
Table 11: EAMSPacketReceiveResponse Layout.....	44
Table 12: EAMSPacketValidationResponse Layout.....	46
Table 13: DWCPacket Layout.....	48
Table 14: Error Codes Blocks To Level Mapping	52
Table 15: Sample Level 1 Error Codes.....	53
Table 16: Sample Level 2 Error Codes.....	53
Table 17: Sample Level 3 Error Codes.....	54

List of Figures

Figure 1 – Bulk Filing – SFTP Flow Diagram.....	9
Figure 2 – DWCPacket – Data Encapsulation Diagram	36
Figure 3 – Submitter – EAMS Payload Exchange Diagram	38
Figure 4 – Canonical Data Model	49

1 Introduction

The Electronic Adjudication Management System (EAMS) was deployed in August 2008.

The original vision for EAMS was to provide all case parties with electronic access to the system via a logon, which gives parties access to eForms as well as documents in the Division of Workers' Compensation's (DWC) case file and other case-related information stored in the case management system. Special Project Report (SPR) 3, submitted in June of 2008, included language calling for additional funding for the provision of greater access to the system for external users. This funding was approved in the provisional language of the budget. Toward that end, the Office of the Chief Information Officer (OCIO) required the Department of Industrial Relations (DIR), DWC's parent agency, and DWC to meet six criteria before the funding would be released.

During the process of meeting the OCIO's requirements, and as a direct result of input from the external user community, the EAMS External User Access Project team recognized that time is a critical factor to user satisfaction in implementation of the EAMS External User Access Project, particularly with respect to the bulk filing capability desired by frequent filers, those who use case management systems and vendors.

Because a very long wait for this capability would not result in the necessary user satisfaction, DIR/DWC's policy is to prioritize its work in a phased manner so that it meets external users' principal needs and minimizes manual processing, while moving toward the goal of full electronic access to EAMS for external users.

The immediate top priority for the division and for external users is efficient electronic filing with minimal manual intervention, which will alleviate lengthy paper processing times.

To fulfill this goal, DIR/DWC has created a "Present Term Solution" (PTS), which will include a new bulk filing mechanism and expanded access to case file information available on the DWC Web site without a logon. This PTS will directly benefit high volume users who are able to immediately take advantage of bulk filing capabilities. The solution will also indirectly benefit other users still filing on paper by reducing the overall volume of paper processed at DWC district offices.

This solution will be implemented as a change request (CR) to the current system and will, therefore, utilize EAMS maintenance and operations personnel.

1.1 Purpose

The purpose of this document is to provide the bulk filing technical specifications required to develop the PTS for both EAMS and submitters' systems.

1.2 Scope

The scope of this document is limited to identifying the bulk filing technical requirements, related business rules and use cases, and data transmission structures. This document also contains detailed design artifacts that will be documented for the design and development of the PTS.

The following related bulk filing topics will be addressed in the next release of this technical specifications document:

- User account creation and management
- User acceptance testing

The Web enhancement technical requirements will be presented in a separate document as they require no technical development for external users.

1.3 References – Documents Reside at New PTS Web Page

The technical documents referenced during the development of this technical specifications document are posted on the new PTS portion of the EAMS Web site. To access the PTS site, go to www.dwc.ca.gov/eams and click on “for bulk filers” under the working in EAMS section.

These technical documents include:

- XML Schemas
- XML Payload Layout Specifications
- Error Codes and Messages
- PTS Terminology Glossary
- SFTP Forms Layout Specifications

2 Present Term Solution (PTS)

The PTS consists of two components:

1. Bulk filing of six priority forms through Secure File Transport Protocol (SFTP), a network methodology standard for securely exchanging encrypted data over the Internet;
2. Expanded access to case file information available on the Web without a logon (this Web enhancement component will be documented in a separate document).

Both of these components are based on needs expressed by external users during requirements gathering sessions and through survey responses.

In short, DIR/DWC will create an SFTP site for bulk filing of six priority EAMS forms, which were chosen because of their status as "[moving documents](#)" and because they are the highest volume forms, which means removing them from the paper queue will yield the best results overall. The EAMS forms are:

- Application for Adjudication of Claim
- Declaration of Readiness to Proceed (to Hearing)
- Declaration of Readiness to Proceed (to Expedited Trial)
- Compromise and Release
- Stipulations with Request for Award
- Notice and Request for Allowance of Lien

This bulk filing mechanism will provide improved submission and error responses to filers by automating error responses related to data entry and editing errors and moving the error "checking" further forward in the document transmission process.

It is important to note that not all errors can be caught up front because of the nature of the EAMS "[batch process](#)".

To assure later compatibility with case management system upgrades and implementation of additional functionality, XML will be utilized for the data transmission stream structures in the PTS.

2.1 SFTP Bulk Filing

2.1.1 Overview

The goal of the SFTP bulk filing component is to address the "must have" (MH) requirements identified by external users in advisory group requirements sessions held in 2009.

Figure 1 below illustrates the SFTP bulk filing mechanism.

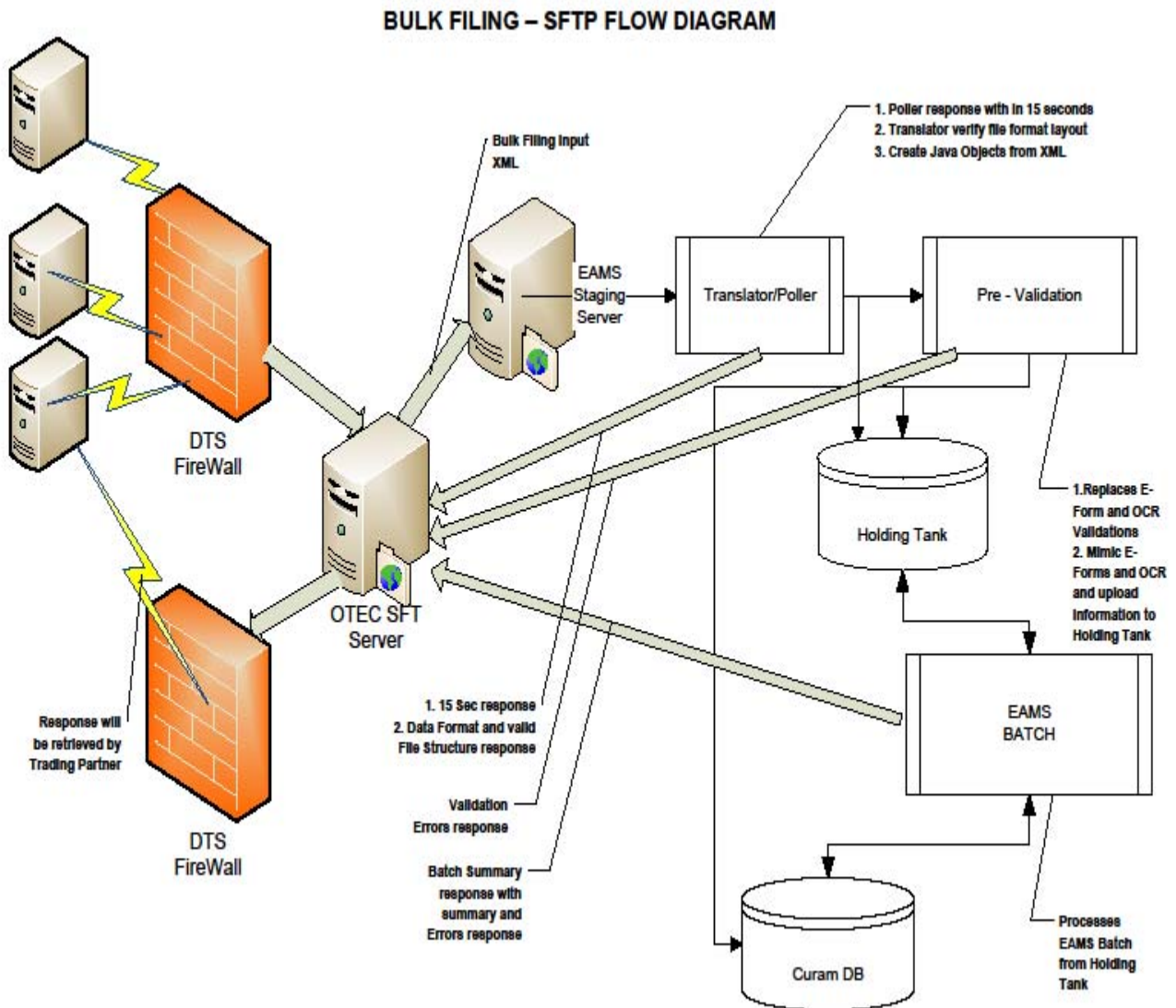


Figure 1 – Bulk Filing – SFTP Flow Diagram

2.2 Present Term Solution – “Must Have” Requirements

This section provides the background for the technical use cases listed in [Section 3.2](#).

The following table lists the 21 “must have” (MH) requirements gathered in the original EAMS External User Access Project process. The table identifies requirement ownership by DIR Office of Information Services (OIS), DWC or the Office of Technology Services (OTech), and whether the requirement is addressed in the PTS.

[Appendix B](#) lists the full business requirements sessions results for historical context.

Original requirement number	High level requirement (HLR) description	Priority: (MH)	Owner	Requirement addressed in PTS
1)	Provide acknowledgment of transmitted submissions and filing status	MH	DIR	YES
3)	Provide notification of planned outages using the system unavailability rule	MH	DWC	YES
4)	Provide a complete summary of all errors contained within the transaction after it has been processed by the EAMS batch interface	MH	DIR	YES
6)	Provide filing capability	MH	DWC/OTech	YES
7)	Define a single standard for connectivity	MH	OTech	
10)	Define standards valid for all submissions	MH	DIR/OTech	YES
10A)	Define industry standard formats to be used for attachments	MH	DIR/DWC	YES
11)	Implement automatic preservation of the original filing date for 15 days (per the rules of administration)	MH	DIR	YES
13)	Provide the capability to support electronic signatures on various incoming documents	MH	DWC/DIR	YES
14)	Implement the functionality to replace the cover sheet and separator sheet with a data header	MH	DWC/DIR	YES
15)	DWC shall develop and provide to all interested parties a detailed list of all data elements, validations and business rules that will be required for successful filing of each DWC and WCAB form to be filed using the systems contemplated in this project	MH	DWC	YES
16)	DWC publishes and maintains a complete list of edits on a form-by-form basis (data element rule)	MH	DWC	YES

Original requirement number	High level requirement (HLR) description	Priority: (MH)	Owner	Requirement addressed in PTS
17)	Form template should be rendered in the same format by the end user and the DWC	MH	DWC	YES
21)	Provide the ability to file additional and amended liens	MH	DWC	
22)	Provide the ability to file documents under seal	MH	DWC/DIR	
24)	Provide a working test environment and minimum standards for external users	MH	OTech	
26)	Provide the capability to protect transmissions to and from the division	MH	OTech	YES
27)	Require security and audit trails for all transactions into DWC	MH	OTech /DIR	YES
29)	Facilitate the filing of the unrepresented QME reports to the DEU	MH	DWC	
38)	Define the rules for 3rd party filers concerning the retention of data and documents filed with 3rd party filers	MH	DWC/OTech	
39)	Provide open solution that is operating system agnostic	MH	OTech	YES

Table 1: EAMS Access "Must Have" Requirements

3 SFTP Bulk Filing Requirements and Technical Use Cases

This section lists the SFTP bulk filing requirements that were captured during EAMS PTS requirements gathering sessions with submitters.

The bulk filing requirements exist in two forms: 1) Business Rules, and 2) Technical Use Cases.

The PTS business rules were developed and refined from the original [“must have” business requirements](#). The technical use cases were developed to guarantee the implementation of the business rules.

3.1 EAMS SFTP Bulk Filing -- Business Rules

3.1.1 EAMS PTS Business Rules

The following table shows the PTS business rules for SFTP bulk filing V2.2 (final), June 8, 2010, which are addressed by the PTS bulk filing component:

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-01	EAMS Hours	SFTP submission shall be done within EAMS operational hours. EAMS hours of operation are as follows: Monday – Wednesday 6:00 a.m. – 8:00 p.m. Thursday 6:00 a.m. – 6:00 p.m. Friday – Saturday 6:00 a.m. – 8:00 p.m. Sunday Closed.	
BR-02	Filing Date	Any document submitted after 5:00 p.m., or on a holiday, Saturday or furlough day, and if processed without error is deemed filed as of the next business day. 8 Cal Code Reg § 10230.	
BR-03	Trading Partner Contact	The submitter will identify in the trading partner agreement a primary and alternate contact person per submitting location and separate email addresses for each. Only these persons may contact the unprocessed document queue (UDQ) operator and/or the EAMS Help Desk. These contacts will also receive notices of planned outages.	See BR-04, BR-12b
BR-04	Notification of Planned Outages	DWC will follow its existing method of notice. That is, email notice will be provided to the SFTP primary and alternate contacts. Notification of planned outages will be sent from the EAMS Command Center (CC) through the Central Registration Unit (CRU) and from CRU to the SFTP trading partner contact.	See BR-03

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-05	Transmission Code Validation	All SFTP trading partners must conduct transmission code testing and receive validation from DIR of their code and upon receipt of validation, their code must be frozen. Any change to trading partner code requires re-validation before filing can continue.	Trading partners not creating their own transmission code must use code that has been validated by DIR.
BR-05a	Validation Prior to Submission	The SFTP submitter must validate the XML to the mandatory field requirements set forth in the form/field spreadsheet.	Software must be programmed to validate the data prior to submission. See BR-10
BR-06	DWC Business Rule and DIR OIS Compliance	Failure to follow DWC business rules and/or DIR Office of Information Services (OIS) requirements may result in revocation of trading partner ability to SFTP file.	
BR-07	Trading Partner Agreements	A completed trading partner agreement must be on file with DWC prior to submitting via SFTP.	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-08	Forms that may be filed by SFTP	Only the following six (6) forms and their appropriate attachments may be filed by SFTP: Application for Adjudication of Claim (Application) Declaration of Readiness to Proceed (DOR) Declaration of Readiness to Proceed to Expedited Hearing (DOR Exp) Notice and Request for Allowance of Lien (Lien) Compromise and Release (C&R) Stipulations with Request for Award (Stips)	See BR-25
BR-09	Format of Attachments	PDF is the preferred format for attachments, but other formats such as TIFF and Word are acceptable. Word Perfect format will not be accepted.	
BR-10	Data Elements, Validations and Business Rules for SFTP Filing	DWC will provide and also publish on its Web site a spreadsheet identifying the fields for each of the six (6) SFTP forms, and whether they are mandatory, conditionally mandatory and/or optionally required for capture in EAMS.	See BR-05a
BR-10a		DWC will post BR-10 spreadsheet on its Web site and DWC alone is responsible for maintaining same. If changes are made to the published version they will be emailed to SFTP trading partner contacts and the updated changes will be listed on the published version on the Web site.	
BR-11	Electronic Filing Exemption	8 Cal Code Reg § 10229. Any OCR filed documents must follow the OCR filing regulations.	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-12	Deletion of Forms and Attachments	The entire form and its attachments will be deleted and the notice of discrepancy will be transmitted to comply with 8 Cal Code Reg § 10222(a)(2) if the form or any of the attachments contain errors such that it will not successfully process into EAMS.	
BR-12a		If more than one form is submitted in a transaction, and one is invalid, only the invalid form and its attachments will be deleted. The valid form(s) and attachments will be processed and the success response will be sent.	The deleted form can be resubmitted once the errors have been corrected.
BR-12b		Archived cases - If the error message "case is archived" is issued, the form and any attachments will be deleted. The submitter's contact person will compile a list of all such case numbers and injured workers' names in Excel format and submit this information in only one (1) email per day to the designated UDQ operator, requesting that they be un-archived. Only after the submitter's contact person receives an email confirmation that the cases are un-archived, may the documents be refiled.	See BR-03
BR-12c		The filing date for deleted forms is governed by 8 Cal Code Reg 10222(a)(2).	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-13	DOR Pending Queue	DOR – If the error message “No suitable slot available” is issued, the DOR and any attachments will be held in the DOR pending queue.	
BR-13a		DORs will be placed in this queue when there are no available slots for the type of hearing requested.	
BR-13b		DORs will be added to the queue chronologically and maintained in date submitted order.	
BR-13c		DORs will be re-processed from the queue in date submitted order once per business day during the first batch process of the day only.	
BR-13d		DORs will remain in the queue for up to fourteen (14) calendar days, being re-processed with the first batch each day the batch process runs. For those DORs still in the queue after fourteen (14) calendar days, the DWC primary and/or alternate SFTP administrator will contact the district office(s) to have them either open hearing slots and/or change the case owner (WCJ), following which the DORs will be re-processed in the next available batch.	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-13e		The DWC primary and/or alternate SFTP administrator will continue to work with the district office(s) for up to five (5) calendar days to successfully re-process the still pending DORs. Should a DOR not successfully process in this time frame, the DOR will be deleted and the submitter notified with a recommendation that the filer submit an OCR walk through DOR.	
BR-14	Form Sequencing	Case opening documents, Application for Adjudication of Claim (Application), Compromise and Release (C&R) or Stipulations with Request for Award (Stips): No other form on the case can be submitted until the notice of application has been issued and received or the filer has confirmed that the C&R or Stips has been received and a case number assigned. [For example, a transaction cannot contain a case opening document form with attachments and a Declaration of Readiness to Proceed (DOR) form on the same case].	
BR-14a		A lien claim has to be successfully filed before a lien claimant or its representative's office can file a DOR requesting a lien conference.	
BR-14b		The SFTP submitter, or the client of a third party SFTP submitter, must be a listed case participant prior to submitting non-case opening documents.	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-14c	Forms that can be Submitted in a Single Transaction	<p>A single transaction is for one (1) case. If the form is a case opening document (Application, Stips, C&R), only that form with its attachments can be in a transaction. Forms that have an existing case number:</p> <p>C&R or Stips - One DOR <u>DOR</u> - A C&R or Stips <u>DOR Expedited</u> - Only the DOR Expedited <u>Lien</u> - One lien per lien claimant, unlimited number of lien claimants</p>	<p>Lien claim example: ABC Medical Clinic, XYZ Transportation, John Bonecutter MD all use the same lien claimant representatives' office which is an SFTP submitter. All 3 of these lien claimants provided services in 1 case - ADJ123456 - all 3 liens can be filed in 1 transaction.</p>

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-15	Digital Signatures	Digital signatures may be used only on the following forms: Application, DOR, DOR Exp, Lien, 10770.5 and 10770.6 verifications as well as any proof of service. The digital signature must be verifiable using the public key for the individual digitally signing the document. The digital signature shall be rebuttably presumed to be that of the individual digitally signing the document when the document is filed using the trading partner name, user ID and password. The trading partner shall bear all costs for development, maintenance and use of the digital signatures. All digital signatures must be valid as of the date affixed to the document and shall be verifiable for the digital signature for a period of ten (10) years from the date of the document on which the digital signature is affixed. The verifiable period of the signature is subject to extension at the discretion of DWC. The public key for each individual digitally signing these documents shall be provided to DWC.	Will not be available at PTS go-live. Phase II of SFTP filing
BR-15a		A digital signature may be added to a document in the following ways: 1) Embedded in the document, in which case the signature is not visible in the signature line. If this method is used, the name of the individual signing the document must be typed on the document signature line 2) Through selection of a visible digital signature, which is affixed to the document.	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-16	S Signatures	S signatures may be used on the following forms: Application, DOR, DOR Exp, Lien, 10770.5 and 10770.6 verifications as well as any proof of service. The s signature shall be rebuttably presumed to be that of the individual whose name is on the document signature line when the document is filed using the trading partner name, user ID and password.	Will be available at PTS go-live. S signature verification NOT required.
BR-16a		S signature must be in the format: S FIRSTNAME LASTNAME: e.g. S JOHN JONES.	
BR-17	Image of Signature	An image of an individual's signature may be used on the following forms: Application, DOR, DOR Exp, Lien, 10770.5 and 10770.6 verifications as well as any proof of service. The image of the signature shall be rebuttably presumed to be that of the individual whose name is on the document signature line when the document is filed using the trading partner name, user ID and password.	Will not be available at PTS go-live. Phase II of SFTP filing
BR-17a		The image must be of the individual's wet/actual signature, scanned and affixed to the document being filed.	
BR-15/16/17b		A digital, s signature or image of a signature is to be used only as noted in BR-15, BR-16 & BR-17, and never on a document requiring a wet/actual signature.	S signature accepted at go-live. Applicable to other signature

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
			methods as they are implemented.
BR-15/16/17c		The rebuttable presumption in BR-15, BR-16 & BR-17 will apply to documents signed digitally, with an s signature or with an image of a signature and filed through an SFTP third party filer (TPF) only if the name of the individual so signing is set forth in the TPF's client list.	S signature accepted at go-live. Applicable to other signature methods as they are implemented.
BR-18	Wet/Actual Signatures	The following documents will require actual wet/actual signature(s) be used: Scanned in signed settlement documents.	The documents requiring a wet/actual signature are attachments to the specific form to which they apply.
BR-19	Additional and Amended Liens	Additional liens will be accepted provided they are filed as "original" (do not use the "amended" field). Amended liens will not be accepted.	
BR19-a	Lien Claims - No Companion Cases	A separate lien claim must filed in each case. Do not list companion cases.	Although the lien itself will be added to FileNet, neither

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
			the lien claimant or lien claimant representative (if listed) will be added to the case participants
BR-20	Documents Under Seal	Any such document(s) must be filed OCR. The presiding judge (PJ) must make determination. 8 Cal Code Reg § 10272.	
BR-21	Current e-filers' Ability to Also File Via SFTP	Current e-filers will be allowed to do both e-forms and SFTP filing. The limitations on OCR filing for e-form trial participants remain in place.	
BR-22	OCR Filing by SFTP Trading Partner	An SFTP trading partner is encouraged to file the six (6) forms by SFTP only. However, OCR filing of these six (6) forms will be allowed.	
BR-22a		SFTP trading partner may file by OCR the designated settlement documents prepared at the district office at the time of a hearing – conference, MSC, trial.	
BR-22b		SFTP filers may submit walk through documents by SFTP filing – C&R and Stips	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-22c		SFTP filers cannot file by SFTP an Amended Application, a Death Application, a C&R Dependency, Stips Death, Third Party C&R, DOR or DOR Expedited for a satellite district office. These must be filed by OCR or via e-form if in the e-form trial or through an authorized e-form TPF.	
BR-23	SFTP Third Party Filer (TPF) Trading Partner Filing Method	The TPF has chosen SFTP as its means of filing the six (6) designated forms. If a client of a TPF wants the TPF to file on its behalf, the TPF is encouraged to file by SFTP. The client does not always thereafter have to file only through the TPF. The client can always file in any manner for which it is authorized; OCR or e-form. Additionally, the TPF may file using any of the means for which it is authorized.	
BR-23a		The TPF's list of clients shall include all individuals' names within its client's organization/office who may be utilizing a digital signature, an s signature or an image of a signature on documents as identified in BR-15-17.	
BR-24	SFTP Office/Individual - Discrete Filer Trading Partner Filing Method	The office/individual has chosen SFTP as its means of filing the six (6) designated forms and is encouraged to only use SFTP to file them, but may file OCR, or via e-form if in the e-forms trial or through an authorized e-form trial third party filer.	This pertains to the discrete filer SFTP trading partner

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-25	Form Packages	Submission of a form must comply with court administrator's regulations regarding completion of fields and filing. The format of the document will use existing business logic as follows in BR-25a-j.	DWC is looking to add appropriate doc types/doc titles for: Venue verification 10770.5 verification 10770.6 verification
BR-25a	Application: Injured Worker or Representatives' Office for Same	In addition to the form, only the following mandatory attachments will be allowed: 4906(g) declaration – if more than one, all scanned in together as a single multi-page document Fee disclosure statement Venue verification Proof of service	
BR-25b	Application: Claims Administrator or Representatives' Office for Same	In addition to the form, only the following mandatory attachments will be allowed: 4906(g) declaration – if more than one, all scanned in together as a single multi-page document Proof of service	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-25c	Application: Lien Claimant or Representatives' Office for Same	In addition to the form, only the following mandatory attachments will be allowed: 4906(g) declaration – if more than one, all scanned in together as a single multi-page document Proof of service – which will include the 10770.5 verification.	
BR-25d	C&R	Only those documents found under 8 Cal Code Reg § 10233 (d)(1) and for walk through, § 10280 – in general, those medical reports specified and documents relevant to a determination of the adequacy of the settlement not filed previously. If the C&R is a case opening document, the appropriate additional document(s) from the "Application" rule are mandatory. Scanned in wet signed C&R - mandatory Proof of service - mandatory	No digital, s, or images of signatures on electronic version of the form.
BR-25e	Stips	Only those documents found under Cal Code Reg § 10233 (d)(1) and for walk through, § 10280 – in general, those medical reports specified and documents relevant to a determination of the adequacy of the settlement not filed previously. If the Stip is a case opening document, the appropriate additional document(s) from the "Application" rule are mandatory. Scanned in wet signed Stips - mandatory Proof of service - mandatory	No digital, s, or images of signatures on electronic version of the form.

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-25f	DOR: Injured Worker, Claims Administrator or Representatives' Office for Same	Can only be filed following receipt of EAMS case number. In addition to the form, only the following attachments will be allowed: Only those documents found in Cal Code Reg § 10233 (b)(1) – a single medical report or if the issue is non-medical, a single document, e.g. earnings, addressing the issue and which have not been filed previously. A rating MSC DOR may require more medical reports than noted above. Proof of service - mandatory.	See BR-13
BR-25g	DOR: Lien Claimant or Representatives' Office for Same	Can only be filed following receipt of EAMS case number. In addition to the form, only the following attachments will be allowed: Only those documents found in Cal Code Reg § 10233 (b)(1) – a single medical report or if the issue is non-medical, a single document, e.g. earnings, addressing the issue and which have not been filed previously. Proof of service – which will include the 10770.6 verification - mandatory.	See BR-13

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-25h	DOR Expedited: Injured Worker or Claims Administrator or Representatives' Office for Same	Can only be filed following receipt of EAMS case number. In addition to the form, only the following attachments will be allowed: Only those documents found in Cal Code Reg § 10233 (c)(1) – a single medical report or if the issue is non-medical, e.g. earnings, a single document addressing the issue not filed previously. Proof of service - mandatory.	
BR-25i	Lien: Lien Claimant or Representatives' Office for Same	Can only be filed following receipt of EAMS case number. In addition to the form, only the following mandatory attachments will be allowed: Itemized billing of charges – An itemized statement is preferred, but if only medical bills exist, all will be scanned in as a single multi-page document Proof of service – which will include the 10770.5 verification.	
BR-26	Legacy Forms	No legacy forms will be accepted.	
BR-27	DWC Pending Queue	Forms, with their attachments, that are otherwise error free but are unable to be processed due to EAMS system issues, will be placed in the DWC Pending Queue.	

Business Rule #	Business Rule Name	Business Rule Description	Business Rule Additional Information
BR-27a		The DWC SFTP administrators will work with the DIR administrators to resolve the EAMS system issue for up to five (5) business days and if resolved, to re-process the form. Should a form not successfully process in this time frame, the form will be deleted and the submitter notified with a recommendation to submit the form via OCR.	
BR-28	Printed Form Format	Forms printed by the submitter must match the format of the existing DWC and WCAB forms	

Table 2: EAMS Business Rules List

3.2 EAMS SFTP Bulk Filing -- Technical Use Cases

EAMS technical [use cases](#) list the set of rules and features that will be the foundation in creating the PTS as described in [Section 2.1](#) and are applicable to the primary actor “EAMS”.

SFTP bulk filing shall be subject to existing EAMS business rules and procedures but may also be subject to additional business rules and procedures as DWC deems necessary.

The following table lists the technical use cases categorized by five high level technical functions/activities that are applicable to the PTS, and are based on the requirements that are defined in [Section 3.1](#) and on the original business use cases found in [Appendix C](#).

3.2.1 Transmission Acknowledgment and Responses

There are three levels of acknowledgment or response to the submitter bulk filing transmissions:

Level 1: Submission acknowledgment simply provides acknowledgment to submitter that the packet was received.

Level 2: Editing response provides notification to submitter of either a successful submission by validating the XML payloads, or of the errors detected in editing.

Level 3: Batch response provides notification to submitter of either the successful acceptance (processing) of a payload into EAMS, or of the errors between submission and EAMS.

Technical Use Case No:	Technical Use Case Statement	Comments
TUC-01	Create and send to submitter an acknowledgment of receipt of packet within 15 seconds of receiving a bulk filing packet from submitter.	Level 1 Acknowledgment
TUC-02	Notify submitter if a duplicate packet is submitted.	Level 1 Acknowledgment
TUC-03	Create and send to submitter acknowledgment details containing whether the packet is accepted successfully for processing or rejected due to one or more errors that include: <ul style="list-style-type: none"> • Mandatory fields that are missing • Invalid data types fields • Invalid field length fields • Any XML errors 	Level 2 Acknowledgment
TUC-04	Create and send to submitter a summary of all transactions that are successfully processed from a packet, with details that include: <ul style="list-style-type: none"> ○ Transaction id ○ case number ○ user defined field ○ Time Stamp ○ document type ○ applicant name 	Level 3 Acknowledgment

Table 3: EAMS Technical Use Cases List – Acknowledgment

3.2.2 EAMS Batch Process

Technical Use Case No:	Technical Use Case Statement	Comments
TUC-05	Retain original date of submission for 15 calendar days in case transaction failed due to validation errors.	
TUC-06	Retain original date of submission for 15 calendar days irrespective of multiple submissions of same transaction to correct errors.	
TUC-07	Identify all errors in a packet.	Will have sub use cases for each type of form.
TUC-08	Process each transaction in a packet.	
TUC-09	Accept transaction with multiple forms and their attachment(s).	
TUC-10	Ensure that the document file date is the submission date.	The submission date is the date the packet is submitted if there are no errors, or the first date the packet is submitted in the 15 calendar day window.
TUC-11	Accept only 6 forms identified in the Present Term Solution as valid SFTP transactions.	
TUC-12	Accept a transaction with multiple forms and their attachment(s) based on business sequencing rules.	
TUC-13	Accept successful form(s) in a transaction if there are no dependencies between the forms submitted when two or more forms are submitted, and there is an error in one or more forms.	
TUC-14	Create error response for the failed form(s) in a transaction when one or more forms are submitted in a transaction.	

Technical Use Case No:	Technical Use Case Statement	Comments
TUC-15	Identify and process resubmission of a form in a transaction if the previous submission resulted in an error and the form is resubmitted within 15 calendar days of its submission.	
TUC-16	Process SFTP solution forms thru existing EAMS business rules routines.	

Table 4: EAMS Technical Use Cases List – EAMS Batch Process

3.2.3 SFTP Transmission

Technical Use Case No:	Technical Use Case Statement	Comments
TUC-17	Accept successful SFTP transmission of a packet from submitter.	
TUC-18	Transmit acknowledgment/responses identified for a packet back to submitter.	
TUC-19	Accept SFTP packet from submitter irrespective of their Operating System thru SFTP protocol.	
TUC-20	Create notification of outages to submitters.	

Table 5: EAMS Technical Use Cases List – SFTP Transmission

3.2.4 Transaction Layouts

Technical Use Case No:	Technical Use Case Statement	Comments
TUC-21	Identify each transaction in a packet.	
TUC-22	Create data stream structures using XML standards.	
TUC-23	Support attachments of various standard formats including PDF, PDF-A, TIFF, GIFF, etc.	
TUC-24	Create the DWCPacket structure to receive incoming transactions, transmit summary report, transmit acknowledgment and transmit errors in transaction.	
TUC-25	Support multiple transactions in a packet submission.	
TUC-26	Support a transaction header data structure that accepts only required fields in the corresponding form cover sheet.	
TUC-27	Support multiple forms in a transaction.	

Table 6: EAMS Technical Use Cases List – Layout

3.2.5 Other Technical Activities

Technical Activity No:	Technical Activity Name	Comments
TA-1	Create user accounts for SFTP for submitters.	
TA-2	Publish error codes and their descriptions.	Available on the PTS web page.

Technical Activity No:	Technical Activity Name	Comments
TA-3	Publish Present Term Solution technical specifications for submitters	Available on the PTS web page.
TA-4	Create a test environment for submitter.	Will be used for User Acceptance testing.

Table 7: EAMS Technical Use Cases List – Others

3.3 Submitter SFTP Bulk Filing -- Technical Use Cases

Submitter technical use cases list the set of rules and features that will be the foundation in creating the solution for the submitter in the PTS as described in [Section 2.1](#)

The following table lists the submitter technical use cases that are applicable to the PTS based on the requirements that are defined in [Section 3.1](#).

Use Case No:	Use Case Statement
UC-01	Register as EAMS Trading partner: <ol style="list-style-type: none"> 1) Connect to EAMS new trading partner account creation site 2) Provide account information 3) Submit request 4) Receive confirmation of submitted request 5) Receive confirmed user account number
UC-02	Create Packet: <ol style="list-style-type: none"> 1) Compile available forms by case 2) Compile relevant attachments for the forms 3) Create XML packet: <ol style="list-style-type: none"> a. Forms of the same case in a transaction b. Multiple transactions in a payload c. Packet or envelope for the payload 4) Validate XML packet against EAMS SFTP Schema

Use Case No:	Use Case Statement
UC-03	<p>Submit Packet to EAMS:</p> <ol style="list-style-type: none"> 1) Open SFTP session using trading partner account 2) Submit packet to designated drop off folder 3) update internal subject claim data with EAMS status of "sent to EAMS"
UC-04	<p>Pickup Level 1 success acknowledgment from EAMS:</p> <ol style="list-style-type: none"> 1) Open SFTP session 2) Identify designated SFTP pickup folder 3) Pickup level 1 receipt file 4) If success, update subject claim data with EAMS status of "received by EAMS" 5) If rejected, identify reject reason and resubmit corrected packet
UC-05	<p>Pickup Level 2 success acknowledgment from EAMS:</p> <ol style="list-style-type: none"> 1) Open SFTP session 2) Identify designated SFTP pickup folder 3) Pickup level 2 receipt file 4) If success, update subject claim data with EAMS status of "Initial Format Accepted by EAMS" 5) If rejected, identify the level 2 errors and resubmit corrected packet
UC-06	<p>Pickup Level 3 success acknowledgment from EAMS:</p> <ol style="list-style-type: none"> 1) Open SFTP session 2) Identify designated SFTP pickup folder 3) Pickup level 3 receipt file 4) If success, update subject claim data with EAMS status of "Accepted by EAMS/DWC"

Table 8: Submitters Technical Use Cases List

4 XML Layout Specifications and Schema Definitions

EAMS will use the DWCPacket layout to receive and send all data streams related to electronic filing of forms by the submitters. The DWCPacket will contain header information and payload information.

The DWCPacket is the master layout that will be used by EAMS and submitter to send and receive all the information related to data streams for SFTP bulk filing as defined in the PTS. The DWCPacket contains a packet header that contains necessary information about the transmitter and payload information. The payload itself will vary based on the layout that will be used.

The figure below describes how the data is encapsulated in DWCPacket:

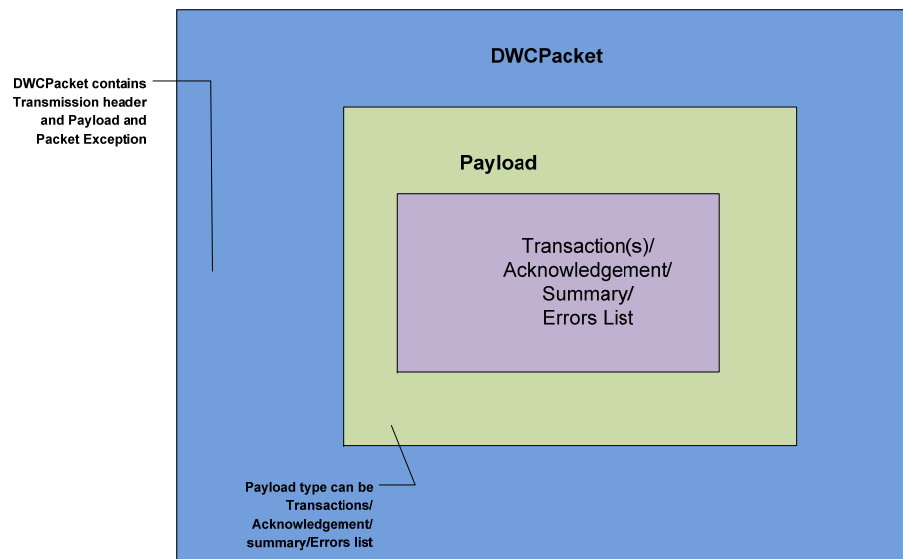


Figure 2 – DWCPacket – Data Encapsulation Diagram

All EAMS responses will send the original packetID back to the submitter along with the response payload information. For the immediate acknowledgment response, the packetID will be extracted from the filename that is submitted.

4.1 Payload Layout

The Payload identifies the business payload that will be sent in the DWCPacket. There will be one payload in a single transmission of the DWCPacket. The payload will vary based on the type of business request and response, either from the submitter or EAMS. For the PTS, the following valid business payloads are identified:

- **SubmitFormsToEAMS** – This payload will be used by the submitter in requesting forms to be processed in EAMS along with their attachments.
- **EAMSFilingResponse** – This payload will be used by EAMS to identify the summary information and errors in the transactions submitted and will be sent by EAMS to submitter.
- **EAMSPacketReceiveResponse** – This payload will be used by EAMS in the initial acknowledgment response, stating that a packet has been received in EAMS. This response will occur within 15 seconds of the packet transmission by the submitter.
- **EAMSPacketValidationResponse** – This payload will be used by EAMS to respond to submitter with all the validation errors that are identified in the packet. Current validations are limited to verifying type of data field and length of data field. For a successful transmission EAMS will respond with “summary” information.

The following figure describes the business payload and the sequence of exchanges between submitter and EAMS:

Submitter – EAMS Payload Exchange Diagram

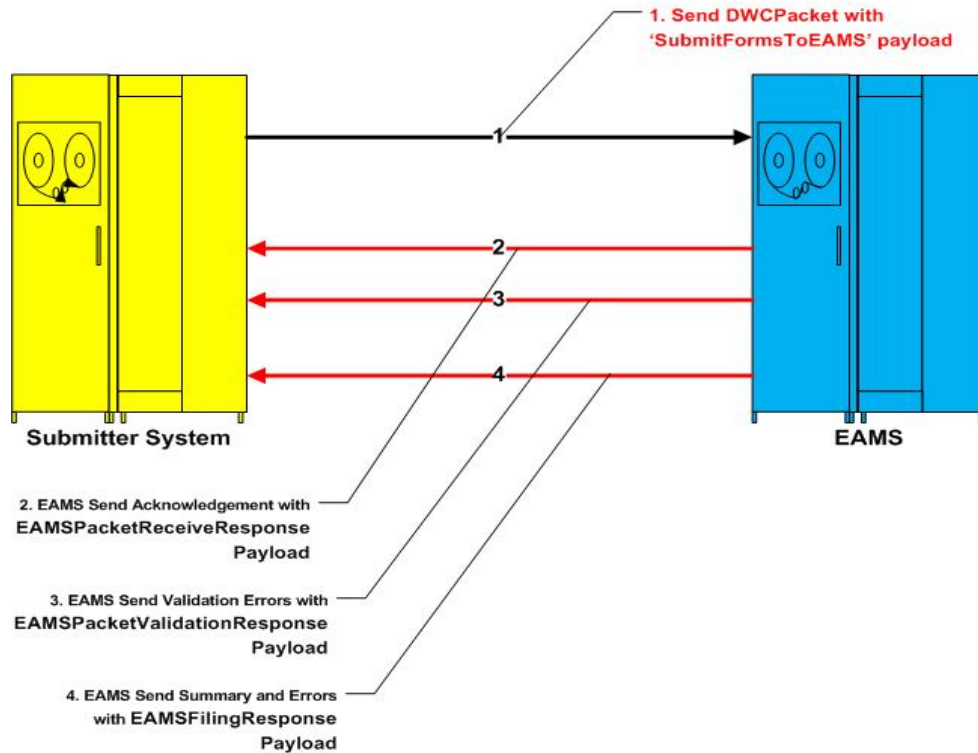


Figure 3 – Submitter – EAMS Payload Exchange Diagram

The EAMS SFTP bulk filing payload layouts include:

- Layout to receive transaction which contains one form header, form data and supporting attachments.
- Layout to send acknowledgment back to submitter after successfully receiving a packet from submitter.
- Layout to send validation errors on a packet back to submitter.
- Layout to send summary data of all successful transactions and errors that will be useful to submitter.

Submitters will use 'SubmitFormsToEAMS' payload to submit forms to be processed in EAMS. All submission files will have a naming convention of '<SERVICENAME>_<PACKETID>'. '<SERVICENAME>' to identify the payload that is submitted. EAMS will accept only 'SubmitFormsToEAMS' as a valid payload. '<PACKETID>' identifies the valid packetID that is submitted.

The following sections describe the layout structures for payloads that will be used in SFTP bulk filing.

4.1.1 SubmitFormsToEAMS Layout

The SubmitFormsToEAMS layout will be used by the submitter to send one or many transactions to EAMS. A transaction is defined as a set of one or more forms and one or more related attachments that are filed for a case. The type of forms that are filed together for a case will depend on business sequencing rules. The transaction will have a transaction header which will be similar to a "CoverSheet" in the existing EAMS system, and one or more forms that will be submitted along with their attachments. There are no restrictions on the number of attachments that can be submitted with a form.

The following layout identifies the groups and fields that will be submitted as a part of SubmitFormsToEAMS service:

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
SubmitFormsToEAMS	VersionNumber	Mandatory			Valid version number
SubmitFormsToEAMS.Transactions		Mandatory			Group (contains one or many transactions)
SubmitFormsToEAMS.Transactions.Transaction		Mandatory			Group
SubmitFormsToEAMS.Transactions.Transaction.Header		Mandatory			Group

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
SubmitFormsToEAMS.Transactions.Transaction.Header	TransactionID	Mandatory	Unique Identifier		Naming Convention: XXXX-DATE-YYYY-ZZZZZ, where: XXXX-ClientId DATE-(Date format: YYYYMMDD) YYYY-RunningSequenceNumber (1..9999) ZZZZZ-RunningSequenceNumber (1...99999)
SubmitFormsToEAMS.Transactions.Transaction.Header.CoverSheet		Mandatory			For fields in coversheet group, refer to Form layout of type coversheet
SubmitFormsToEAMS.Transactions.Transaction.Forms		Mandatory			Group (contains one or many forms)
SubmitFormsToEAMS.Transactions.Transaction.Forms.Form		Mandatory			Group
SubmitFormsToEAMS.Transactions.Transaction.Forms.Form	FormID	Mandatory			Unique Form type
SubmitFormsToEAMS.Transactions.Transaction.Forms.Form	FormSequenceNumber	Mandatory			Unique Form Sequence Number, will be a positive running sequence number within the transaction, starting from 1
SubmitFormsToEAMS.Transactions.Transaction.Forms.Form	ResubmissionIndicator	Mandatory	Y, N	N	Resubmission indicator

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
SubmitFormsToEAMS.Transactions.Transaction.Forms.F orm	ResubmissionID	Optional			ResubmissionID generated by EAMS
SubmitFormsToEAMS.Transactions.Transaction.Forms.F orm	FormData	Mandatory			This maps to the form schema based on the form ID.
SubmitFormsToEAMS.Transactions.Transaction.Forms.F orm.Attachments		Optional			Group (contains one or many attachments)
SubmitFormsToEAMS.Transactions.Transaction.Forms.F orm.Attachments.Attachment		Mandatory			
SubmitFormsToEAMS.Transactions.Transaction.Forms.F orm.Attachments.Attachment	AttachmentTitle	Mandatory			Document Title
SubmitFormsToEAMS.Transactions.Transaction.Forms.F orm.Attachments.Attachment	AttachmentName	Mandatory			Document Name
SubmitFormsToEAMS.Transactions.Transaction.Forms.F orm.Attachments.Attachment	AttachmentBase64	Mandatory			Attachment encoded using Base64 encoding

Table 9: SubmitFormsToEAMS Payload Layout

4.1.2 EAMSFilingResponse Layout

The EAMSFilingResponse layout will be used by EAMS to send a response containing summary data for successful transactions processed, and an error section detailing the transactions that failed in EAMS batch processing. The failed transactions contain the error codes and error message details. There can be an instance where a transaction will appear on both the summary and error sections. This will happen when more than one form is submitted and not all the forms are successfully processed. For example, two forms submitted out of sequence, as defined by the business rules, will cause this outcome.

The following layout identifies the groups and fields that will be sent back from EAMS as a part of EAMSFilingResponse service:

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
EAMSFilingResponse	VersionNumber	Mandatory			Valid version number
EAMSFilingResponse.Summary		Mandatory			Group
EAMSFilingResponse.Summary.Transactions		Mandatory			Group (contains one or many transactions)
EAMSFilingResponse.Summary.Transactions.Transaction		Mandatory			Group
EAMSFilingResponse.Summary.Transactions.Transaction	TransactionID	Mandatory			Will be returned from the Original submission
EAMSFilingResponse.Summary.Transactions.Transaction	DateSubmitted	Mandatory			Will be returned from the Original submission
EAMSFilingResponse.Summary.Transactions.Transaction.Forms		Mandatory			Group (contains One or many form)
EAMSFilingResponse.Summary.Transactions.Transaction.Forms.Form		Mandatory			Group
EAMSFilingResponse.Summary.Transactions.Transaction.Forms.Form	FormID	Mandatory			Unique Form type
EAMSFilingResponse.Summary.Transactions.Transaction.Forms.Form	FormSequenceNumber	Mandatory			Will be returned from the Original submission
EAMSFilingResponse.Summary.Transactions.Transaction.Forms.Form	FiledDate	Mandatory			
EAMSFilingResponse.Summary.Transactions.Transaction.Forms.Form	CaseNumber	Mandatory			
EAMSFilingResponse.Summary.Transactions.Transaction.Forms.Form	ResubmissionIndicator	Mandatory	Y,N	N	Resubmission indicator

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
EAMSFilingResponse.Errors.Transactions		Mandatory			Group (contains One or many transaction)
EAMSFilingResponse.Errors.Transactions.Transaction		Mandatory			Group
EAMSFilingResponse.Errors.Transactions.Transaction	TransactionID	Mandatory	Unique Identifier		Will be returned from the original submission
EAMSFilingResponse.Errors.Transactions.Transaction.Forms		Mandatory			Group (contains One or many form)
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm		Mandatory			Group
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm	FormID	Mandatory			Will be returned from the original submission
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm	FormSequenceN umber	Mandatory			Will be returned from the original submission
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm	ResubmissionID	Mandatory			Unique resubmission ID generated by EAMS
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm.Errors		Mandatory			Group (one or many form errors)
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm.Errors.Error		Mandatory			Group
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm.Errors.Error	ErrorCode	Mandatory			
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm.Errors.Error	ErrorPrimary	Mandatory			
EAMSFilingResponse.Errors.Transactions.Transaction.Forms.F orm.Errors.Error	ErrorSecondary	Mandatory			

Table 10: EAMSFilingResponse Layout

4.1.3 EAMSPacketReceiveResponse Layout

The EAMSPacketReceiveResponse layout will be used by EAMS to send an acknowledgment back to submitter that a packet is received.

The following layout identifies the group and field that will be submitted as part of the EAMSPacketReceiveResponse service:

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
EAMSPacketReceiveResponse	VersionNumber	Mandatory			Valid version number
EAMSPacketReceiveResponse	Message	Mandatory			

Table 11: EAMSPacketReceiveResponse Layout

4.1.4 EAMSPacketValidationResponse Layout

The EAMSPacketValidationResponse layout will be used by EAMS to send an acknowledgment back to submitter that a packet is validated successfully.

The following layout identifies the groups and fields that will be submitted as a part of EAMSPacketValidationResponse service:

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
EAMSPacketValidationResponse	VersionNumber	Mandatory			Valid version number
EAMSPacketValidationResponse	Acknowledgment	Mandatory			
EAMSPacketValidationResponse.Errors		Optional			Group
EAMSPacketValidationResponse.Errors.Transactions		Mandatory			Group (contains one or many transactions)
EAMSPacketValidationResponse.Errors.Transactions.Transaction					Group
EAMSPacketValidationResponse.Errors.Transactions.Transaction	TransactionID	Mandatory	Unique Identifier		Will be returned from the original submission
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms		Optional			Group (contains one or many forms)
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form		Mandatory			Group
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form	FormID	Mandatory			Will be returned from the original submission
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form	FormSequence Number	Mandatory			Will be returned from the original submission
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form.FormErrors		Mandatory			Group (one or many form errors)
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form.FormErrors.FormError		Mandatory			Group
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form.FormErrors.FormError	ErrorCode	Mandatory			
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form.FormErrors.FormError	ErrorPrimary	Mandatory			

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form.FormErrors.FormError	ErrorSecondary	Mandatory			
EAMSPacketValidationResponse.Errors.Transactions.Transaction.Forms.Form	ResubmissionID	Mandatory			Unique resubmission ID generated by EAMS
EAMSPacketValidationResponse.Errors.Transactions.TransactionErrors		Optional			Group
EAMSPacketValidationResponse.Errors.Transactions.TransactionErrors.TransactionError		Mandatory			
EAMSPacketValidationResponse.Errors.Transactions.TransactionErrors.TransactionError	ErrorCode	Mandatory			
EAMSPacketValidationResponse.Errors.Transactions.TransactionErrors.TransactionError	ErrorPrimary	Mandatory			
EAMSPacketValidationResponse.Errors.Transactions.TransactionErrors.TransactionError	ErrorSecondary	Mandatory			

Table 12: EAMSPacketValidationResponse Layout

4.2 DWCPacket Layout

The following table describes the fields in the DWCPacket layout:

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
DWCPacket	VersionNumber	Mandatory			Valid version number
DWCPacket.DWCPacketHeader		Mandatory			Group
DWCPacket.DWCPacketHeader	PacketID	Mandatory	Unique Identifier		Naming Convention:

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
					XXXX-DATE-YYYY XXXX- ClientUserId Date-Date(YYYYMMDD) YYYY- RunningSequenceNumber (1..9999)
DWCPacket.DWCPacketHeader	TransportProtocol	Mandatory	SFTP		FTP is the only protocol
DWCPacket.DWCPacketHeader	PacketType	Mandatory	REQ/REP/ERR		Request - Input Reply - Summary Message Exception - Errors
DWCPacket.DWCPacketHeader	ClientUserId	Mandatory			(SFTP userid)
DWCPacket.DWCPacketHeader	SecurityToken	Optional			
DWCPacket.DWCPacketHeader	TestMessage	Optional	TRUE/FALSE	FALSE	Whether to ignore processing
DWCPacket.DWCPayloadInformation		Mandatory			Group
DWCPacket.DWCPayloadInformation	ServiceName	Mandatory	IN1/OU1/OU2/OU3		UniqueServiceNames IN1 - SubmitFormsToEAMS, OU1 - EAMSFilingResponse, OU2 - EAMSPacketReceiveResponse, OU3- EAMSPacketValidationResponse
DWCPacket.DWCPayloadInformation	ServiceVersion	Mandatory			Valid version number
DWCPacket.DWCPayloadInformation	PayloadFormat	Mandatory	XML	XML	This maps to the Data Model that will be used for exchange
DWCPacket.DWCPayloadInformation	PayloadSchema	Optional			Schema Name
DWCPacket.DWCPacketHeaderSource		Mandatory			Group
DWCPacket.DWCPacketHeaderSource	LogicalSystem	Mandatory			Submitters System -

Group/Field	Field	Required	Acceptable Values - Bulk Filing	Default Value - Bulk Filing	Comments
					company system name
DWCPacket.DWCPacketHeaderSource	Environment	Mandatory	DEV/TST/UAT/PRD		'DEV' - Development, 'TST' - Test, 'UAT' - User Acceptance, 'PRD' - Production
DWCPacket.DWCPacketHeaderTarget		Mandatory			Group
DWCPacket.DWCPacketHeaderTarget	LogicalSystem	Mandatory	EAMS		
DWCPacket.DWCPacketHeaderTarget	Environment	Mandatory	DEV/TST/UAT/PRD		'DEV' - Development, 'TST' - Test, 'UAT' - User Acceptance, 'PRD' - Production
DWCPacket	DWCPacketPayload	Mandatory			Valid Payload
DWCPacket.DWCPacketExceptions		Optional			Group (contains one or many exception)
DWCPacket.Exceptions.Exception		Mandatory			Group
DWCPacket.DWCPacketExceptions.Exception	ErrorCode	Mandatory	Error Codes		
DWCPacket.DWCPacketExceptions.Exception	ErrorPrimary	Mandatory	high level message		Primary message mapping to the code
DWCPacket.DWCPacketExceptions.Exception	ErrorSecondary	Mandatory			Detail secondary message

Table 13: DWCPacket Layout

4.3 Forms Specifications

Refer to SFTP Forms Layout Specification v2.0 in [Appendix E](#).

4.4 Canonical Data Model

EAMS Forms Canonical Data Model organizes all the form field elements and their domain. The following figure illustrates the mapping between various data models and the EAMS Form Canonical Data Model that are discussed in the PTS.

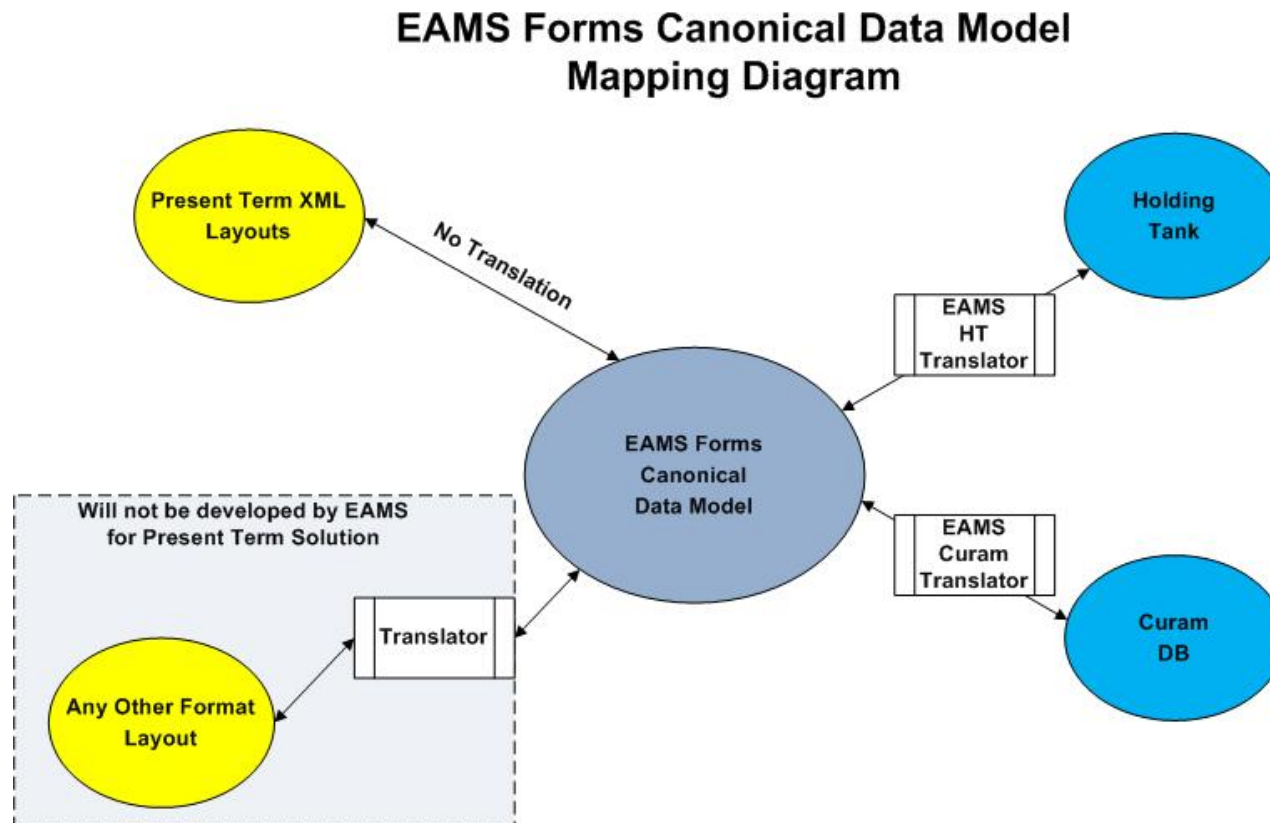


Figure 4 – Canonical Data Model

The EAMS PTS XML Layouts field definitions will be identical to the EAMS Forms Canonical Data Model. So when a submitter transmits the DWCPacket using the PTS layout definition, EAMS will accept the transmission and process the transmission data that is submitted using the EAMS HT Translators and EAMS Cúram Translator.

When a submitter chooses to use an XML layout definition that is not identical to the EAMS Forms Canonical Data Model, the submitter must develop a translator to convert it to the standard DWCPacket layout format. EAMS will not develop translators to accept any other format of input transmission (example: 2GEFS format) that are not identical to the EAMS Forms Canonical Data Model.

The following mappings are identified for the EAMS Canonical Model in the Present Term Solution:

- Forms Layout Fields to Canonical Fields Mapping
- Holding Tank to Canonical Fields Mapping
- Cúram to Canonical Fields Mapping

The EAMS Forms Canonical Data Model specifications are for EAMS DIR OIS internal use only. Submitters will use the schema specifications defined in Appendix E to create the bulk filing “SubmitFormsToEAMS” payload and receive transmission acknowledgments, errors, and summary information payloads for the submitted SFTP bulk filing.

4.5 Schema Definitions

Refer to schema downloadable zip [SchemasComplete](http://www.dir.ca.gov/dwc/EAMS/PresentTermSolution/Schemas/CompleteSchema)
<http://www.dir.ca.gov/dwc/EAMS/PresentTermSolution/Schemas/CompleteSchema>.

5 Error Codes and Messages

Error messages are categorized into three different groups to be sent to the submitter when an input transmission is received. The three error message groups map to the three levels of acknowledgment or response that will be sent back to the submitter (see [Section 3.2.1](#)).

Following are the three levels of acknowledgment or response:

- Level 1: Submission acknowledgment simply provides submitter with acknowledgment that the packet was received.
- Level 2: Editing response provides notification to submitter of either a successful submission by validating the XML payloads, or of the errors detected in editing.
- Level 3: Batch response provides notification to submitter of either the successful acceptance (processing) of a payload into EAMS, or of the errors between submission and EAMS.

EAMS will include both the error code and error message in the summary/exception responses. When errors are detected in the submitter's payload, they are mapped to the relevant error code and error message in the PTS Error Codes and Messages Table (see [Section 5.4](#)) and sent back to the submitter.

The PTS Error Codes and Messages Table is organized by error code, and a “primary” error message and a “secondary” detailed error message for each error code. The primary error message groups error messages by type. The secondary error message provides the detailed error message which gives a description of the error and includes the section and field name where applicable.

The “secondary” detailed error message is formatted in one of two ways:

- As a general error statement, e.g.:
for error code 10020, “Invalid DWCPacket version.”
- OR, when a field name and value is required in the error response:
- As an error statement containing <SectionName>.<FieldName>.<Field Value>, e.g.:

for error code 20050, "<SectionName>.<FieldName>.<Field Value> Case Number found for Case Opening Document."

OR

- As an error statement containing <FieldName>.<Field Value>, e.g.:
for error code 20090, "<FieldName>.<Field Value> S Signature Format Incorrect."

The following table defines the error codes numbering blocks that will be used:

Error Code Blocks	Level	Description
10000	Level 1	Error codes that are packet related will be thrown in level 1.
20000	Level 2	Validation errors that are related to formatting of XML and any conditional field validation.
30000	Level 3	Batch processing errors.

Table 14: Error Codes Blocks To Level Mapping

5.1 Level 1 Error Messages

A Level 1 error message will be generated if there is a problem with the submitted packet. As noted above, Level 1 errors generate "10000" error code values. The following table lists a sample of the Level 1 error messages:

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with	FIELD NAMES
------------	------------------------	--	-------------

		field element values)	
10010	DWCPacket Schema Format Errors	<FieldName>.<Field Value> Schema Field format error.	All fields.

Table 15: Sample Level 1 Error Codes

5.2 Level 2 Error Messages

Level 2 error messages will be generated if there is a problem validating the input XML structure and entering the data into the Holdingtank (HT) database (staging area). There should be minimal Level 2 errors because the XML schema validations will catch most of the invalid data field lengths and data type errors.

Level 2 errors generate “20000” error code values. The following table lists a sample of the Level 2 error messages:

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
20060	Schema Errors	<SectionName>.<FieldName>.<Field Value> Schema Field format error.	All fields.

Table 16: Sample Level 2 Error Codes

5.3 Level 3 Error Messages

Level 3 error messages will be generated during batch processing, when the submitter’s payload is loaded into EAMS. Level 3 errors generate “30000” error code values. The following table lists a sample of the Level 3 error messages:

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
30000	DOR Filing Error For Lien Conference.	No Lien found for the case.	

Table 17: Sample Level 3 Error Codes

5.4 Error Codes and Messages Table

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
10000	DWCPacket Transmission Errors	1) Invalid File Name. 2) Duplicate PacketID found.	
10010	DWCPacket Schema Format Errors	<FieldName>.<Field Value> Schema Field format error.	All fields.
10020	Invalid DWCPacket Value	1) PacketID doesn't match with FileName. 2) Invalid DWCPacket version. 3) Invalid ClientUserId specified. 4) Invalid Payload ServiceName. 5) Invalid Payload ServiceVersion. 6) Invalid Target.LogicalSystem. 7) Invalid Target.Environment.	

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
20000	Invalid Date Value	<p>1) <SectionName>.<FieldName>.<Field Value> must be later than the date of injury <Field Value>.</p> <p>2) <SectionName>.<FieldName>.<Field Value> must be earlier than the date of injury <Field Value>.</p> <p>3) <SectionName>.<FieldName>.<Field Value> must be later or equal to the date of birth <Field Value>.</p> <p>4) <SectionName>.<FieldName>.<Field Value> must be earlier or equal to current date.</p> <p>5) <SectionName>.<FieldName>.<Field Value> date is too far in the past (can't exceed 130 years earlier than current date).</p> <p>6) <SectionName>.<FieldName>.<Field Value> must be equal to or later than the date of injury <Field Value>.</p>	<p>1) DOR.DateOfSignature, DORExpedited.DateOfSignature, DOR.DateOfDoctorReport</p> <p>2) <AllForms> DateOfBirth</p> <p>3) AppForADJ.DateOfInjuryStart, CompromiseAndRelease.DateOfInjuryStart, Stips.DateOfInjuryStart, DOR.DateOfSignature, DORExpedited.DateOfSignature</p> <p>4) <AllForms>DateOfBirth, AppForADJ.DateOfInjuryStart, CompromiseAndRelease.DateOfInjuryStart, Stips.DateOfInjuryStart, NoticeAndRequestOfLien.DateOfOriginalLien, NoticeAndRequestOfLien.DateOfSignature, DORExpedited.DateOfSignature</p> <p>5)<AllForms>. DateOfBirth, AppForADJ.DateOfInjuryStart, CompromiseAndRelease.DateOfInjuryStart, Stips.DateOfInjuryStart</p> <p>6) AppForADJ.DateOfSignature, NoticeAndRequestOfLien.DateOfOriginalLien, NoticeAndRequestOfLien.DateOfSignature</p>
20010	Invalid Date Sets	<SectionName>.<FieldName>.<Field Value> must be later than <SectionName>.<FieldName>.<Field Value>.	<p>AppForADJ.DateOfInjuryEnd ~ AppForADJ.DateOfInjuryStart, CompromiseAndRelease.DateOfInjuryEnd ~ CompromiseAndRelease.DateOfInjuryStart, NoticeAndRequestOfLien.DateOfInjuryEnd ~ NoticeAndRequestOfLien.DateOfInjuryStart, Stips.DateOfInjuryEnd ~ Stips.DateOfInjuryStart</p>

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
20020	Conditional Mandatory	<p>1) AppForADJ Missing DateOfInjuryEnd, which is required if InjuryType is "C"(Cumulative).</p> <p>2) AppForADJ Missing ClaimsAdministrator, which is required when Employer is insured or self insured or legally uninsured.</p> <p>3) AppForADJ Insurance Carrier must be blank when Employer is self insured or legally uninsured.</p> <p>4) AppForADJ ClaimsAdministrator and Insurance Carrier must be blank when Employer is uninsured.</p> <p>5) AppForADJ Missing S Signature, must have either Applicant Attorney/Representative Signature or Applicant Signature.</p> <p>6) CompromiseAndRelease Missing Injury Information for a case opening document.</p> <p>7) CompromiseAndRelease Missing ClaimsAdministrator, which is required when Employer is insured or self insured or legally uninsured.</p> <p>8) CompromiseAndRelease Insurance Carrier must be blank when Employer is self insured or legally uninsured.</p> <p>9) CompromiseAndRelease ClaimsAdministrator and Insurance Carrier must be blank when Employer is uninsured.</p> <p>10) Stips Missing Injury Information for a case opening document.</p>	

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
		<p>11) Stips Missing ClaimsAdministrator, which is required when Employer is insured or self insured or legally uninsured.</p> <p>12) Stips Insurance Carrier must be blank when Employer is self insured or legally uninsured.</p> <p>13) Stips ClaimsAdministrator and Insurance Carrier should be blank when Employer is uninsured.</p> <p>14) NoticeAndRequestOfLien Missing S Signature, must have either Lien Claimant Attorney/Representative Signature or Lien Claimant Signature.</p> <p>15) NoticeAndRequestOfLien Missing Lien request reason.</p> <p>16) DOR Missing principal issues.</p> <p>17) DORExpedited Missing declarant request reason.</p> <p>18) CoverSheet Walkthru Indicator (true) valid only for CompromiseAndRelease, Stips.</p>	

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
20030	Invalid Uniform Assigned Name	<SectionName>.<FieldName>.<Field Value> UAN not found in EAMS.	
20040	Resubmission Errors	1) Invalid Resubmission ID for the form ID. 2) Resubmission indicator missing.	
20050	Case Number Errors	1) <SectionName>.<FieldName>.<Field Value> Case Number found for Case Opening Document. 2) <SectionName>.<FieldName>.<Field Value> Companion Case(s) listed on a Lien Claim. 3) <SectionName>.<FieldName>.<Field Value> Companion Case listed for AppForADJ case opening document. 4) <SectionName>.<FieldName>.<Field Value> Invalid Case Number format. 5) <SectionName>.<FieldName>.<Field Value> Invalid Companion Case Number format. 6) <SectionName>.<FieldName>.<Field Value> Case Number not found in EAMS. 7) <SectionName>.<FieldName>.<Field Value> Companion Case Number not found in EAMS. 8) <SectionName>.<FieldName>.<Field Value> Invalid Case Number for Injured Worker. 9) <SectionName>.<FieldName>.<Field Value> Invalid Companion Case Number for Injured Worker.	
20060	Schema Errors	<SectionName>.<FieldName>.<Field Value>	All fields.

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
		Schema Field format error.	
20070	Invalid Field Code Value Error	<SectionName>.<FieldName>.<Field Value> Invalid Code.	AppForADJ.BodyPart, CompromiseAndRelease.BodyPart, Stips.BodyPart, AppForADJ.VenueLocationCode, CompromiseAndRelease.VenueLocationCode, Stips.VenueLocationCode, AppForADJ.VenueOfficeCode, CompromiseAndRelease.VenueOfficeCode, Stips.VenueOfficeCode, AppForADJ.EmployerRoleTypeCode, CompromiseAndRelease.EmployerRoleTypeCode, Stips.EmployerRoleTypeCode, AppForADJ.AttorneyorAuthRepTypeCode, CompromiseAndRelease.AttorneyorAuthRepTypeCode, Stips.AttorneyorAuthRepTypeCode, NoticeAndRequestOfLien.AttorneyorAuthRepTypeCode, AppForADJ.InjuryType, CompromiseAndRelease.InjuryType, Stips.InjuryType
20080	Invalid Injured Worker	No match found for the Injured Worker's last name, date of birth, date of injury or SSN.	On non-case opening document.
20090	S Signature Errors	<FieldName>.<Field Value> S Signature Format Incorrect.	
20100	SubmitFormsToEAMS Schema Format Errors	<FieldName>.<Field Value> Schema Field format error.	
20110	SubmitFormsToEAMS Invalid Payload Error	1) Invalid Version Number. 2) Invalid TransactionID. 3) Duplicate TransactionID. 4) Duplicate FormSequenceNumber.	

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
		5) Invalid FormSequenceNumber.	
20120	Invalid Form Version	<FormName><FieldName>.<Field Value> Invalid version number.	
20130	Mandatory Attachment Not Found.	<p>1) AppForADJ filed by Injured Worker or Representative. <AttachmentName>.</p> <p>2) AppForADJ filed by Claims Administrator or Representative. <AttachmentName>.</p> <p>3) AppForADJ filed by Lien Claimant or Representative. <AttachmentName>.</p> <p>4) CompromiseAndRelease (non case opening). <AttachmentName>.</p> <p>5) CompromiseAndRelease (case opening). <AttachmentName>.</p> <p>6) Stips (non case opening). <AttachmentName>.</p> <p>7) Stips (case opening). <AttachmentName>.</p> <p>8) DOR filed by Injured Worker, Claims Administrator or Representative. <AttachmentName>.</p> <p>9) DOR filed by Lien Claimant or Representative. <AttachmentName>.</p> <p>10) DORExpedited <AttachmentName>.</p>	<p>1) 4906(g) Declaration, Fee Disclosure Statement (only for App filed by Representative), Venue Verification, Proof of Service.</p> <p>2) 4906(g) Declaration, Proof of Service.</p> <p>3) 4906(g) Declaration, Proof of Service which will include the 10770.5 verification.</p> <p>4) Scanned in wet signed CompromiseAndRelease, Proof of Service.</p> <p>5) Scanned in wet signed CompromiseAndRelease, Proof of Service, the appropriate additional document(s) from the "Application" rule.</p> <p>6) Scanned in wet signed Stips, Proof of Service.</p> <p>7) Scanned in wet signed Stips, Proof of Service, the appropriate additional document(s) from the "Application" rule.</p> <p>8) Proof of Service.</p> <p>9) Proof of service with 10770.6 verification.</p> <p>10) Proof of Service.</p>

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
		11) NoticeAndRequestOfLien <AttachmentName>.	11) Proof of Service.

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
20140	Invalid Attachment Found In Transaction	<p>1) AppForADJ filed by Injured Worker or Representative. <SectionName>.<FieldName>.<Field Value>.</p> <p>2) AppForADJ filed by Claims Administrator or Representative. <SectionName>.<FieldName>.<Field Value>.</p> <p>3) AppForADJ filed by Lien Claimant or Representative. <SectionName>.<FieldName>.<Field Value>.</p> <p>4) CompromiseAndRelease (non case opening). <SectionName>.<FieldName>.<Field Value>.</p> <p>5) CompromiseAndRelease (case opening). <SectionName>.<FieldName>.<Field Value>.</p> <p>6) Stips (non case opening). <SectionName>.<FieldName>.<Field Value>.</p> <p>7) Stips (case opening). <SectionName>.<FieldName>.<Field Value>.</p> <p>8) DOR filed by Injured Worker, Claims Administrator or Representative. <SectionName>.<FieldName>.<Field Value>.</p> <p>9) DOR filed by Lien Claimant or Representative. <SectionName>.<FieldName>.<Field Value>.</p> <p>10) DORExpedited. <SectionName>.<FieldName>.<Field Value>.</p> <p>11) NoticeAndRequestOfLien</p>	

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
		.<SectionName>.<FieldName>.<Field Value>.	
20150	DWC Pending Queue	Form has been sent to DWC Pending Queue. Disposition pending.	
30000	DOR Filing Error For Lien Conference.	No Lien found for the case.	
30010	DOR Queue	DOR pending.	

ERROR CODE	ERROR MESSAGE(Primary)	ERROR MESSAGE DETAILS (Secondary) (This field will be part of error message and contain details on the sub category of the error message with field element values)	FIELD NAMES
30020	DWC Pending Queue	Form has been sent to DWC Pending Queue. Disposition pending.	
30030	File By OCR	Form cannot be processed – file by OCR.	

6 Present Term Solution (PTS) Security

Security for the PTS ensures that data exchanged between EAMS and the trading partners are kept safe. DIR/DWC is concerned with infrastructure security, which deals with data in flight and at rest.

This aspect of security must be assured both for the bulk filing data that is transmitted via SFT accounts and also for the sensitive administrative data that is sent and received by account management service (AMS) staff for SFT accounts.

6.1 SFT Overview

EAMS will utilize a Secure File Transport (SFT) system for file exchanges with the trading partner. The external trading partner will log into the SFT and that will establish a secure tunnel for the transmission of data. SFT ensures that data is safe through SSH encryption (aka Secure Shell) while it's in flight (or during transfer). The information the trading partner is sending to EAMS is kept safe because:

1. Username, passwords and commands are encrypted, so logon and command information are not readable by others.
2. The data being sent to EAMS are also encrypted and not readable by others.

6.2 Infrastructure Security – Office of Technology Services (OTech) Security Standard

Once the data has been transferred, infrastructure security makes sure that data at rest (the trading partner data that has been received by the PTS) is safe. OTech is the State of California's data center. OTech hosts some of the largest state agency systems, such as DMV and EAMS. They are data center security experts, and they maintain strict security standards to protect the State's data. OTech's standard for file transfer is Secure File Transport (SFT), which is behind a firewall that protects the production environment. The data stored on the SFT is encrypted with Triple Data Encryption Standard (DES) in memory. Triple DES has been approved by the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) for encrypting sensitive government information.

6.3 Infrastructure Security – Present Term Solution

PTS and EAMS are hosted at OTech and adhere to the OTech security standard (http://www.servicecatalog.dts.ca.gov/docs/3117_Network_Architecture_Standard.pdf). The SFT system meets the OTech security standard. PTS will leverage SFT as its file

transport mechanism. To protect the data, all files sent will be secure at all times. First, the data is protected by SFTP protocol (using SSH) while the data is being transmitted to SFT. Once the files are received by SFT they are encrypted with Triple DES in memory. The files will be decrypted and moved to the secure EAMS environment for processing, all behind the OTech firewalls.

7 Guidelines and Standards

7.1 Technical Guidelines

The following guidelines are intended to further qualify and explain the technical information and specifications presented in this document. The guidelines are grouped into categories of greatest interest to facilitate the submitters' access to useful information. Submitters can take advantage of the guidelines to help them submit and receive successful SFTP bulk filing transmissions.

7.1.1 Form Guidelines

The following section describes the general edits and validations for forms that must be enforced by the submitter when submitting forms. The complete list of fields related to the validations can be found in the PTS bulk filing Error Codes and Messages Table (see [Section 5.4](#)).

1. Date field values must be later than the date of injury wherever applicable.
2. Date field values must be equal to or later than the date of injury wherever applicable.
3. Date field values must be later than date of birth wherever applicable.
4. Date field values must be earlier or equal to current date wherever applicable.
5. Date of Birth value can't exceed 130 years earlier than current date.
6. Date set values supplied must be valid; e.g. - start date should be earlier than end date.
7. Fields which use codes must have valid values.
8. Law Firm or Representative Name must be a Uniform Assigned Name (UAN).
9. Claims Administrator must be a Uniform Assigned Name (UAN).
10. S Signature format must be "S FIRST NAME LAST NAME" e.g. "S JOHN JONES".
11. Mandatory attachments must be attached for each form.
12. Invalid attachments must not be submitted for a form.
13. Latest version of the form schema layout is the valid version.

14. Submitted injured worker information for a non-case opening form must match what exists in EAMS.
15. Only valid schema data elements must be submitted.
16. Valid Resubmission ID must be listed along with Resubmission Indicator when a form is resubmitted for previous error.
17. Date of Injury Start and Date of Injury End are required if Injury Type is "C" (Cumulative).
18. Claims Administrator information must be supplied when Employer is insured or self insured or legally uninsured in AppForADJ, CompromiseAndRelease, Stips forms.
19. Insurance Carrier information must be blank when Employer is self insured or legally uninsured in AppForADJ, CompromiseAndRelease, Stips forms.
20. Both Claims Administrator and Insurance Carrier information must be blank when Employer is uninsured in AppForADJ, CompromiseAndRelease, Stips forms.
21. AppForADJ form must have either Applicant Attorney/Representative S Signature or Applicant S Signature.
22. NoticeAndRequestOfLien forms must have either Attorney/Representative S Signature or Lien Claimant S Signature.
23. Injury Information must be supplied for CompromiseAndRelease and Stips forms when they are to be treated as case opening documents.
24. Principal issues must be submitted for DOR form.
25. Declarant request reason must be submitted for DOR Expedited form.
26. CoverSheet Walkthru Indicator (true) valid only for CompromiseAndRelease, Stips

7.1.2 Transaction Guidelines

The following section describes the general edits and validations for a transaction that must be enforced by the submitter when submitting transactions. The complete list of fields related to the validation can be found in the PTS bulk filing Error Codes and Messages Table (see [Section 5.4](#)).

1. Case Number must not be listed on case opening document forms.
2. Companion Case(s) must not be listed on the AppForADJ case opening document form.

3. Case Numbers and Companion Case Numbers must be of right format.
4. Valid EAMS Case Numbers and Companion Case Numbers must be supplied for an injured worker.
5. Valid version of the transaction schema layout must be submitted.
6. Duplicate transaction must not be submitted.
7. Valid Transaction ID must be submitted
8. Valid Transaction must be submitted – Case opening document can not be submitted with a non case opening document.
9. Valid schema data elements must be submitted.

7.1.3 Payload Guidelines

The following section describes the general edits and validations for a payload that must be enforced by the submitter when submitting a payload. The complete list of fields related to the validation can be found in PTS bulk filing Error Codes and Messages Table (see [Section 5.4](#)).

1. Valid version of the transaction schema layout must be submitted.
2. Valid schema data elements must be submitted.

7.1.4 Transmission and DWCPacket Guidelines

The following section describes the validations that must be enforced by the submitter when submitting a file. The complete list of fields related to the validations can be found in PTS bulk filing Error Codes and Messages Table (see [Section 5.4](#)).

1. Valid file name must be submitted.
2. Valid Payload Service Name and Service Version must be submitted.
3. Valid Target information must be submitted.
4. Duplicate file must not be submitted.
5. Duplicate Packet_ID must not be submitted.

6. Valid version of the DWCPacket schema layout must be submitted.

7.1.5 Exception Handling Guidelines

The following section describes the EAMS response for handling errors in a transmission. The complete list of fields related to the validations can be found in PTS bulk filing Error Codes and Messages Table (see [Section 5.4](#)).

1. EAMS will reject a file if any of the validations identified in [Section 7.1.3](#), [Section 7.1.4](#) fail.
2. EAMS will reject a transaction if any of the validations identified in [Section 7.1.2](#) fail.
3. EAMS will error a form in a transaction if any of the validations identified in [Section 7.1.1](#) fail.
4. EAMS will track the original date of submission for a form if the file submitted is valid and the transaction for the form is valid.
5. EAMS will generate a Resubmission ID for errored forms. This ID will be used by the submitter to submit errored forms if the original submission date needs to be preserved.

7.2 XML Schema Standards

The following sections describe the standards that were followed in creating XML schema layouts for SFTP bulk filing.

SFTP bulk filing XML schema layouts were created based on W3C standards (XML Schema: Structures Second Edition, W3C Recommendation 28 October 2004, and URL: http://www.w3.org/TR/xmlschema-1/#cElement_Declarations). Data types, usage of groups, complex types were modeled on W3C standards.

XML form field names and element names were modeled based on ebXML Technical Architecture Specification v1.0.4 (URL: <http://www.ebxml.org/specs/ebTA.pdf>). The standards followed include.

- All Element names start with a Capital Letter – example SocialSecurityNumber and follow UCC (UpperCamelCase) naming convention.
- All simpleType field names will start with a small letter – socialSecurityNumber and follow LCC (lowerCamelCase)
- No spaces, dashes or other punctuation marks will be used.

The following sub sections describe the schema standards which were followed during schema development.

7.2.1 General Schema Guidelines

1. Elements that branch off the root will end in “Section”. Example: ApplicationSection, EmployerSection.
2. General rules for all names are:
 - A. Acronyms and Abbreviations are not used. Example VenueLocationCode is used instead of VenueLocationCd
 - B. Underscore (_), periods (.) and dashes (-) are not used. Example VenueLocationCode is used instead of Venue_Location_Code/ Venue-Location-Code/ Venue.Location.Code

7.2.2 Standard Elements

Standard elements and complex types are reused in defining form structure wherever applicable. Some of the standard structures are

- Address – used wherever an address is required (AddressLine1, City, State & Zip)
- Venue – used wherever a Venue Location and Venue Office is required
- Name – used wherever a Person’s name is required.

7.2.3 Field Restrictions

Standard field restrictions are applied across all forms wherever applicable. The field restrictions may not follow standard OCR template field restrictions or E-form template field restrictions. Some of the standards are

- addressLine1 is restricted to 40 UpperCase characters A to Z, digits 0 to 9, and special characters ' # space
- city is restricted to 25 UpperCase characters A to Z, and special characters - ' space
- firstName is restricted to 25 UpperCase characters A to Z, and special character -
- fullAddress is restricted to 40 UpperCase characters A to Z, digits 0 to 9, and special characters ' # space
- fullLongName is restricted to 80 UpperCase characters A to Z, and special characters ' –

- lastName is restricted to 25 UpperCase characters A to Z, and special characters '-'
- middleInitial is restricted to 1 UpperCase characters A to Z
- organizationName is restricted to 56 UpperCase characters A to Z, and special characters '-' space
- phoneNumber is restricted to 10 digits 0 to 9
- socialSecurityNumber is restricted to 9 digits 0 to 9
- zip5Code is restricted to 5 digits 0 to 9
- Any dollar value must be between 0 and a max of 99999999999999.99

7.2.4 Section Names

Section names were created to group logical set of form elements. The section names and grouping of fields may not follow the standard OCR template or eForm template. Some of section name examples include

- ApplicationSection
- ApplicantSection
- EmployeeSection

Appendix A: PTS Project Terminology/Descriptions

Terminology	Description	Source
GENERAL SOFTWARE-NETWORK-DATA TRANSMISSION TERMS		
Artifact	An artifact is one of many kinds of tangible byproducts produced during the development of software. Some artifacts (e.g., use cases , class diagrams , and other UML models, requirements and design documents) help describe the function, architecture, and design of software. Other artifacts are concerned with the process of development itself - such as project plans, business cases, and risk assessments.	http://en.wikipedia.org/wiki/Artifact_(software_development)
Bandwidth	The amount of information or data that can be sent over a communications channel in a given period of time. The higher a channel's bandwidth, the more information it can carry.	http://www.toolingu.com/definition-450270-39852-data.html
Boundary	The separation point between network segments. Boundaries are usually set by devices that control the data, such as routers and gateways.	http://www.toolingu.com/definition-450270-39852-data.html
Carrier sense	The ability of a network device to "listen" to the network to determine if any other devices are trying to transmit data.	http://www.toolingu.com/definition-450270-39852-data.html
Carrier sensing multiple access with collision detection	An Ethernet communication protocol in which devices check the network to see if it is clear before transmitting data.	http://www.toolingu.com/definition-450270-39852-data.html
Collision	A situation in which two or more network devices send data at the same time.	http://www.toolingu.com/definition-450270-39852-data.html
Collision detection	The ability of network nodes to sense when there is a collision. When collisions occur, the nodes simply wait to re-transmit the information.	http://www.toolingu.com/definition-450270-39852-data.html

Terminology	Description	Source
Data	Information is transmitted or processed digitally. In data transmission, a “1” or “0” represents the most fundamental unit of information in a digital system.	http://www.toolingu.com/definition-450270-39852-data.html
Firewall	A piece of hardware or software that protects a network from unwanted content or unauthorized users.	http://www.toolingu.com/definition-450270-39852-data.html
Header	Supplemental data placed at the beginning of a block of data being stored or transmitted.	http://en.wikipedia.org/wiki/Header_(computing)
Industry standard	A universally accepted set of guidelines for the operational quality of a device or process.	http://www.toolingu.com/definition-450270-39852-data.html
Infrastructure	The physical equipment that makes up the network. The most important part of network infrastructure is the transmission medium.	http://www.toolingu.com/definition-450270-39852-data.html
Input/output device	A device connected to the input/output section of a computer. Inputs are usually sensors while outputs are usually devices that perform a mechanical action.	http://www.toolingu.com/definition-450270-39852-data.html
Interface	An Interface in Computer science refers to a set of named operations that can be invoked by clients. Interface generally refers to an abstraction that an entity provides of itself to the outside.	http://en.wikipedia.org/wiki/Interface_(computer_science)
Megabit	One million bits. A bit is a single numerical unit in the binary number system.	http://www.toolingu.com/definition-450270-39852-data.html
Metadata	Metadata is “data about data”.	http://en.wikipedia.org/wiki/Metadata
Message	The instructions contained in a data packet.	http://www.toolingu.com/definition-450270-39852-data.html
Moving document	A document that requires action.	
Multiple access	A type of network access in which each node on the network has the same right to transmit data packets as any other node.	http://www.toolingu.com/definition-450270-39830-multiple-access.html
Packet	A unit of data that carries information such as instructions. TCP/IP is a communications	http://www.toolingu.com/definition-450270-39852-data.html

<i>Terminology</i>	<i>Description</i>	<i>Source</i>
	protocol that breaks data up into packets.	
Protocol	The standards and rules used by computers and other network devices to interact with each other. In many respects, protocols are the language that network devices use to communicate.	http://www.toolingu.com/definition-450270-39852-data.html
Router	A network device that determines where information packets should go and sends them to their destination by the shortest, most efficient route.	http://www.toolingu.com/definition-450270-39852-data.html
SFTP	SSH File Transfer Protocol , a network protocol designed to provide secure file transfer and manipulation facilities over SSH .	http://en.wikipedia.org/wiki/SFTP
Switch	A network hardware device that allows different nodes on the network to communicate with each other. Switches have the ability to selectively forward data packets to a specific destination.	http://www.toolingu.com/definition-450270-39852-data.html
Transmission	Transfer of files across a network.	
Transmission error	An error on the transmission network.	
Transmission medium	The means by which data travels through a network. Typically this is some type of cable, although wireless networks are becoming increasingly common.	
PRESENT TERM SOLUTION PROJECT TERMS		
Batch process	A process that runs within EAMS to move transactions from the Holding Tank to appropriate	EAMS Definition.

<i>Terminology</i>	<i>Description</i>	<i>Source</i>
	databases.	
Bulk filing	The ability to file multiple EAMS Forms and related attachments in a single electronic transmission.	EAMS Definition.
Digital signature	An electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature. (See chapter 10 of title 2, division 7 of Cal. Code of Regs., 2 CCR § 22000, et seq.).	Cal. Code of Regs
DWCPacket	The DWCPacket is the master layout that will be used by EAMS and submitter to send and receive all the information related to data streams for SFTP bulk filing as defined in the "Present Term Solution" technical specification.	Present Term Solution technical specifications
Electronic signature	An electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. (This definition is based on section 106 of the federal E-SIGN Act. 15 USCS § 7006).	Section 106 of the Federal E-SIGN Act. (15 USCS § 7006)
Error response	The response from DWC to the submitter about errors contained in a bulk filing transaction.	Present Term Solution technical specifications
Form	The six EAMS forms used in the Present Term Solution. The forms are: -Application for Adjudication of Claim -Declaration of Readiness to Proceed (to hearing) -Declaration of Readiness to Proceed (to Expedited Trial) -Compromise and Release -Stipulations with Request for	Present Term Solution technical specifications

<i>Terminology</i>	<i>Description</i>	<i>Source</i>
	Award -Notice and Request for Allowance of Lien.	
Form header	A data record within a packet that includes the high level form information of the bulk filing .	Present Term Solution technical specifications
Form trailer	A data record within a packet that includes information such as last modified date, character encoding, sender name, transaction ID and more.	Present Term Solution technical specifications
Packet	A Packet is the transmission of a payload which has 1 or more transactions; a transaction is for one case and the transaction has 1 or more forms and attachments.	Present Term Solution technical specifications
Packet header	A data record within a packet that includes the high level information of the bulk filing .	Present Term Solution technical specifications
Packet trailer	A data record within a packet that includes information such as last modified date, character encoding, sender name, transaction ID and more.	Present Term Solution technical specifications
Payload	Material transmitted over a network (either computer or telecommunications network) includes both data and information that identifies the source and destination of the material. The payload is the actual data, or the cargo, carried by the headers .	http://en.wikipedia.org/wiki/Payload_(communication_and_information_technology)
S signature	Signature of filer on the form in the format of S JOHN JONES.	
S signature verification	Verification signed by the person whose S Signature is on the form – the required language to be provided by DWC.	
Submitter	Any one of the external user participants in the “Present Term Solution” project.	Present Term Solution technical specifications
Transaction	Within a bulk filing, the data representation of one case that has 1 or more forms and	Present Term Solution technical specifications

<i>Terminology</i>	<i>Description</i>	<i>Source</i>
	attachments.	
Transaction error	An error in the format of the transaction.	Present Term Solution technical specifications
Transaction error response	The response from DWC to the submitter whose transaction contained errors.	Present Term Solution technical specifications
Transaction header	A data record within a packet that includes the high level transaction information of the bulk filing .	Present Term Solution technical specifications
Transaction trailer	Information such as last modified date, character encoding, sender name, transaction ID and more.	Present Term Solution technical specifications
UDQ	Unprocessed Documents Queue	
Use case	A use case in software engineering and systems engineering is a description of a system's behavior as it responds to a request that originates from outside of that system. In other words, a use case describes "who" can do "what" with the system in question. The use case technique is used to capture a system's behavioral requirements by detailing scenario-driven threads through the functional requirements .	http://en.wikipedia.org/wiki/Use_case

Appendix B: EAMS Access Business Requirements List

<http://www.dir.ca.gov/dwc/ForumDocs/EAMSPresentTermSolutionDocumentRepository/EAMS%20access%20project%20high%20level%20business%20requirements.pdf>

Appendix C: EAMS Access Business Use Case Statements

<http://www.dir.ca.gov/dwc/ForumDocs/EAMSPresentTermSolutionDocumentRepository/EAMS%20access%20external%20user%20submitted%20use%20case%20statements.pdf>

Appendix D: SFTP Forms-ID Mapping

FORM ID	FORM
10232_1	Coversheet (but this is being changed to a transaction header)
WCAB_1	Application for Adjudication o Claim
10214_a	Stipulations with Request for Award
10252_1	Declaration of Readiness to Proceed (expedited trial)
WCAB_6	Notice and Request for Allowance of Lien
10250_1	Declaration of Readiness to Proceed
10214_c	Compromise and Release

Appendix E: SFTP Forms Layout Specifications

<http://www.dir.ca.gov/dwc/EAMS/PresentTermSolution/PresentTermSolution.htm>